

EXHIBIT 5



**TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

**APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL**

In the Matter of the Search of
AN APPLE IPHONE 8 BEARING SERIAL
NUMBER F4HVL9LMJ, CURRENTLY
LOCATED AT JOHN F. KENNEDY
INTERNATIONAL AIRPORT, EVIDENCE
STORAGE ROOM

20-M-187

Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ ☒

Name: Robert M. Pollack

Firm Name: USAO-EDNY

Address: 271-A Cadman Plaza East

Brooklyn, NY 11201

Phone Number: 718.254.6232

E-Mail Address: robert.pollack@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ☒

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: ___; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

February 24, 2020

DATE

SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____

Judge/Magistrate Judge: _____

Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Integrity of ongoing investigation of criminal conspiracy; potential subjects at large.

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK
February 24, 2020

Robert Levy

U.S. DISTRICT JUDGE/U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE February 24, 2020
DATE

BELLIOISI_00463

BELLOISI 00464

Case No.:
20-M-187

Copy of warrant and inventory left with:

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

PH:RMP
F.#2020R00153

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE 8 BEARING SERIAL
NUMBER F4HVL9LMJ, CURRENTLY
LOCATED AT JOHN F. KENNEDY
INTERNATIONAL AIRPORT, EVIDENCE
STORAGE ROOM

TO BE FILED UNDER SEAL

Case No. 20-M-187

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, JOHN M. MOLONEY, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I have participated in numerous investigations of narcotics smuggling and distribution involving international airports, and specifically the smuggling of controlled substances in and through John F. Kennedy International Airport (“JFK”). I have also received training on the uses and capabilities of cellular devices.

3. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; and from reports of other law enforcement officers involved in the investigation.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. As set forth in Attachment A, the property to be searched is an Apple iPhone 8 bearing serial number F4HVL9LMJ, hereinafter the “Device.” The Device is currently located in the Evidence Storage Room at JFK Building 75, Suite 217, Jamaica, NY 11430.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On February 4, 2020, at approximately 3:36 p.m., American Airlines flight 1349 from Montego Bay, Jamaica arrived at JFK Terminal 8. Immediately thereafter, two Customs and Border Patrol (“CBP”) officers who are members of the JFK Anti-Terrorism Contraband Enforcement Team began an enforcement exam of the aircraft, which includes, among other things, an inspection of external aircraft panels and the main avionics compartment, which is on the underside of the aircraft beneath and behind the cockpit. Upon searching the avionics compartment, Officer-1 discovered ten “bricks” of a substance that appeared to be cocaine concealed behind an insulation blanket on the port side of the compartment.

8. Officer-1 and Officer-2 (collectively, the “Officers”) removed the suspected contraband and replaced it with “sham” bricks. They sprayed the sham bricks and insulation blanket that concealed them with a substance that glows when illuminated with certain light, and placed an electronic transponder that would send a radio signal if the area around the sham bricks was disturbed. The Officers then left the aircraft, and along with HSI agents began visual surveillance of the underside of the aircraft from a distance.

9. For several hours, the Officers observed no activity near the avionics compartment and the transponder was not tripped. The aircraft was scheduled to depart for its next flight at 8:00 p.m. Approximately 20 to 30 minutes before that scheduled departure, after the aircraft had already begun boarding the next flight, the Officers observed an American Airlines mechanic entering the avionics compartment. The Officers would later learn that this mechanic was PAUL BELLOISI.

10. Within 3-5 seconds after BELLOISI entered the compartment, the transponder was “tripped,” sending a signal to the officers that the area around the sham bricks had been disturbed. Officer-1 and Officer-2, along with a supervisory CBP officer and an acting deputy chief, drove from the observation area to the aircraft. Officer-1 and Officer-2 approached the avionics compartment and observed BELLOISI re-adjusting and securing the insulation blanket that had formerly concealed the suspected contraband.

11. In my training and experience, the recipients of contraband smuggled in aircraft compartments often receive information from co-conspirators concerning the quantity or appearance of the contraband in advance of shipment. Such information, often transmitted by

telephone or other electronic means, facilitates the receipt of contraband and the detection of changes caused by the interception of the contraband by law enforcement.

12. It is my professional assessment that the reason BELLOISI was observed re-adjusting and securing the insulation blanket that had formerly concealed the suspected contraband rather than removing the sham contraband is likely that he had already received information, by telephone or otherwise, about the quantity or appearance of the contraband that he was intended to receive, and he was therefore able to detect the sham contraband by discrepancies between it and the real contraband that it replaced.

13. BELLOISI began to descend from the avionics compartment and the officers confronted him. The gloves that BELLOISI was wearing glowed when illuminated under a certain light, providing another indication to the Officers that BELLOISI had touched or handled the area where suspected contraband had previously been concealed. The Officers advised BELLOISI that he was being detained for questioning by HSI.

14. The Officers observed that the “tug” vehicle that BELLOISI had driven to the aircraft, and which was parked near the avionics compartment, contained an empty red tool bag, pictured below, in plain view.



15. Another HSI special agent and I transported BELLOISI to the Joint Narcotics Smuggling Unit. While there, BELLOISI removed his American Airlines jacket, and I subsequently observed that the inside lining of the jacket had been cut or sliced in the chest area

on both sides, forming inside “pockets” in the interior lining of the jacket, as depicted in the photographs below.



16. In my training and experience, narcotics smugglers commonly make such cutouts to carry concealed contraband in the interior lining of coats and jackets. The red tool bag and the interior jacket lining together would have been sufficient to carry the seized contraband.

17. The seized contraband was field tested with positive results for cocaine. The total quantity seized was 11.594 kilograms (25.560 pounds).

18. BELLOISI was arrested and his personal effects were seized and inventoried. The Device was among these personal effects. The Device is thus currently in the lawful possession of HSI, having come into HSI's possession when it was seized incident to BELLOISI'S arrest. Therefore, while HSI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.¹

¹ In the course of my training and experience, I have become aware that numerous federal courts "have found probable cause to search cellphones possessed by defendants arrested in connection with ongoing drug-distribution crimes based on the experience of agents familiar with narcotics trafficking that traffickers commonly use cellphones to communicate in the course of their narcotics distribution, as well as to store relevant information, including the names and contact information of suppliers, purchasers, and confederates." United States v. Hoey, No. 15-CR-229 (PAE), 2016 WL 270871, at *9 (S.D.N.Y. Jan. 21, 2016); see also United States v. Robinson, No. 16-CR-545 (ADS), 2018 WL 5928120, at *16 (E.D.N.Y. Nov. 13, 2018) (citing cases); United States v. Barrett, 824 F. Supp. 2d 419, 449 (E.D.N.Y. 2011) (probable cause found based on facts indicating defendant was involved in drug trafficking and agent's declaration that "(1) cell phones are capable of electronically storing numerous types of information; and (2) in her experience, individuals involved in narcotics trafficking typically use cellular phones to communicate and store information and other records on their phones").

19. The Device is currently in storage at the Evidence Storage Room at JFK Building 75, Suite 217, Jamaica, NY 11430. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For

example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device; movements prior to the intended receipt of contraband, including movement to and from meetings with co-conspirators, and to the site intended for the receipt of contraband; and communications, photographs, audio recordings, or Internet searches that reveal details of a drug trafficking conspiracy.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

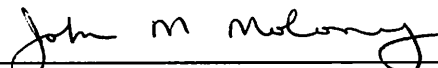
CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING


27. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation of a criminal drug trafficking conspiracy, not all of whose participants are known or will be searched at this time. Based upon my training and experience, I have learned that people engaged in criminal conspiracies often search for affidavits and search warrants via the internet, and may seek to use information about ongoing investigations to destroy evidence or tamper with potential witnesses. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



JOHN M. MOLONEY
Special Agent
Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me
on February 24, 2020:



THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

As set forth in Attachment A, the property to be searched is an Apple iPhone 8 bearing serial number F4HVL9LMJ, hereinafter the “Device.” The Device is currently located in the Evidence Storage Room at JFK Building 75, Suite 217

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. §§ 952, 960, and 963 and involve PAUL BELLOISI and any co-conspirators since January 4, 2020, including:

- a. communications, photographs, videos, notes or sound recordings related to American Airlines flight 1349, or otherwise related to the February 4, 2020 transportation and importation of cocaine;
- b. communications, photographs, videos, notes or sound recordings related to drug trafficking or importation;
- c. any information related to the identities of BELLOISI's co-conspirators (including names, addresses, phone numbers, or any other identifying information);
- d. any Internet or search history relating to drug trafficking;
- e. lists of customers and related identifying information;
- f. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- g. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- h. any information recording BELLOISI's or his co-conspirators' schedule or travel from January 4, 2020 to the present;

- i. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
 - a. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the law enforcement agents may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.